Strategy Research Project

BLUE FORCE TRACKING: BUILDING A JOINT CAPABILITY

BY

LIEUTENANT COLONEL MICHAEL M. SWEENEY
United States Marine Corps

USAWC CLASS OF 2008

U.S. Army War College, Carlisle Barracks, PA 17013-5050

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
15 MAR 2008	**Strategy Research Project**	**00-00-2007 to 00-00-2008**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Blue Force Tracking: Building a Joint Capability	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
Michael Sweeney	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	8. PERFORMING ORGANIZATION REPORT NUMBER
U.S. Army War College ,122 Forbes Ave.,Carlisle,PA,17013-5220	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT
see attached

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**Same as Report (SAR)**	**30**	

The U.S. Army War College is accredited by the Commission on Higher Education of the Middle State Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

USAWC STRATEGY RESEARCH PROJECT

BLUE FORCE TRACKING: BUILDING A JOINT CAPABILITY

by

Lieutenant Colonel Michael M. Sweeney
United States Marine Corps

Colonel David A. Kelley
Project Adviser

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

ABSTRACT

AUTHOR: Lieutenant Colonel Michael M. Sweeney

TITLE: Blue Force Tracking: Building a Joint Capability

FORMAT: Strategy Research Project

DATE: 1 March 2008 WORD COUNT: 5,980 PAGES: 29

KEY TERMS: Blue Force Situational Awareness, Combat Identification

CLASSIFICATION: Unclassified

Blue Force Tracking technology is a battle proven force enabler desired by commanders at all echelons. The ability to know who an individual or unit is, and where they are located will continue to be a critical need in the rugged environments of the future. The realities of current operations have created such a need for this capability, and there are at least a dozen different devices being used in our current operations supporting all functional areas. This has created interoperability challenges in that none of the disparate systems are able to share data amongst themselves without additional technical processing and distribution. Development of a joint capability is required for tomorrow's fight that resolves the peer to peer data sharing issues while reducing the burden on satellite assets. Success will take leadership, strategy, and resources. It is a coherent strategy that is most needed to develop a capability that is born and developed jointly.

BLUE FORCE TRACKING: BUILDING A JOINT CAPABILITY

Blue Force Tracking (BFT) capabilities have been heralded as critical in helping to build situational awareness (SA) on the battlefield. They have become an important tool in today's battlespace. Commanders at all echelons have complimented the capabilities that this technology brings and its importance as a joint force enabler. So important is the capability, that within the Department of Defense (DoD) alone, the plan is to grow the number of devices from about 50,000 in use today, to over 250,000 by 2015.[1] This does not account for the requirement when interagency and multinational partners are factored in. Despite the importance of tracking friendly forces and the anticipated growth in this area, a holistic approach on how to proceed in the development of a true joint capability is lacking. The devices in use today bring various capabilities from a number of manufacturers, most of which are incapable of sharing the blue force data they generate with different platforms on a "peer to peer" basis. Technical solutions and procedures that allow for the exchange of BFT generated information have been developed, but the ability to see all device inputs on a common operational picture is proving to be a challenging endeavor.[2] This complicates not only force tracking and command and control, but also critical tactical operations such as clearing fires.

The complexity of warfare, increasing reliance on technology, and realities of the joint environment highlight the need for a strategy that will allow for the development of a joint capability in this critical area. Failure to address issues that present themselves today in the form of policy, standards, infrastructure, procurement, and training will complicate efforts to leverage this technology in the future. This analysis will frame the

issues at hand, evaluate available options, and offer specific recommendations for building a joint capability.

Clarifying Terms

To gain an appreciation of the challenges that exist, it is first necessary to outline the vernacular that is used when discussing BFT. The Chairman of the Joint Chiefs of Staff (CJCS) describes BFT as the "employment of techniques to actively or passively identify and track US, allied, or coalition forces for the purpose of providing enhanced battlespace situational awareness."[3] BFT devices generally can be categorized as one-way (beaconing) instruments that have the ability to send data only, or two-way instruments that can both send and receive ''blue" and other data that provides a level of situational awareness as well as some ability to command and control (C2).

One-way BFT devices simply determine **where** a friendly unit is located, and **who** the friendly unit is. The data used to determine where the unit is consists of time, latitude, longitude, and altitude information obtained from an embedded Global Positioning System (GPS) (this information can also be obtained from other position reporting systems). The GPS obtained information is normally referred to as Position Location Information (PLI), and that, combined with pedigree information associated with the specific transmitting device is commonly referred to as a 'track.'[4]

Two-way devices generate this data as well, but also have the ability to provide **status** and **intent** information. Blue Force Situational Awareness (BFSA) is the collection and integration of capabilities provided by systems or tracking devices and transmission mediums employed to obtain, report, and share Blue Force Identification.[5] Situational Awareness (SA) is the coupling of situational development (interpreting the

battlespace through all available input mechanisms) and situational assessment. BFT and BFSA contribute to situational development but not entirely, nor do they provide a full assessment of friendly forces or other elements that commanders must take into consideration.

Some have come to see BFT as a way to reduce fratricide. One could argue that BFT informs the Combat Identification (CID) process, but BFT devices are not designed to reduce fratricide as CID systems are.[6] BFT contributes to SA, and that coupled with target identification forms the foundation for shoot, no-shoot decisions that CID systems are designed to facilitate. Figure 1 shows the nested relationships between BFT, BFSA, SA, and CID.[7]

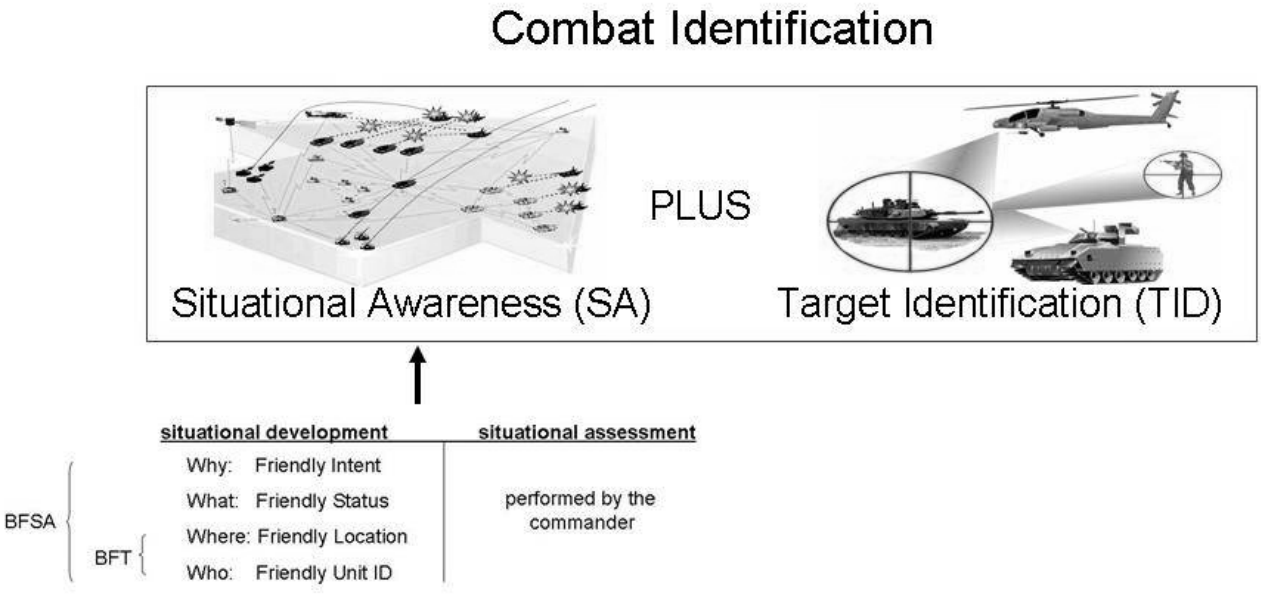

Figure 1.

Although this analysis is not intended to evaluate specific tracking devices or systems, the various types and increasing numbers have in fact created interoperability challenges. Although most of the challenges have been highlighted through the

extensive use of BFT by the U.S. Army, U.S. Marine Corps, and special operations units, all Services, Combatant Commanders (CCDRs), and joint organizations share equity in overcoming the obstacles at hand. At least twelve different BFT/BFSA systems are being used in operations ongoing in Iraq and Afghanistan. This capability has proven to have applicability in virtually every functional warfighting area, but the majority of devices are segregated in such a way that they align with particular mission domains, or functions, and their unique operating requirements.[8] Brief descriptions are provided below.

Conventional force BFT systems generally provide BFSA capabilities to tactical forces. System displays plot a variety of markers on area maps including blue force positions and status, known red force positions, engagement locations, and comprehensive messaging capabilities. This can best be described as the digitized version of the hard copy maps with acetate overlays in combat operation centers of old. Conventional force systems are designed to operate in either a classified or unclassified mode.

Logistics BFT systems track logistics vehicles and containers utilizing both one-way and two-way communications. They normally utilize commercial-based satellite services that operate at the unclassified level.

Special Operations Forces (SOF) and Other Government Agency (OGA) systems provide tracking of personnel, with an emphasis on secure Limited Probability of Intercept (LPI) and Limited Probability of Detection (LPD) tracking. This ensures that the location of SOF and OGA personnel are not compromised. The majority of these systems employ a beaconing capability associated with one-way communications and

only limited two-way communications in the form of brevity codes. The communications architecture supporting these devices operate at the classified level.

Personnel Recovery (PR) BFT systems operate at the classified level and provide tracking and messaging to individual persons needing rescue. They are only used in the event that a rescue is needed and are not activated during missions by default. They are used extensively in the aviation community for pilot rescue.[9]

The alignment of functionality with mission domain makes sense from a requirements perspective provided the devices developed and procured are able to share data and information. That is not the case today.

The BFT System

A BFT system consists of more than just the tracking device. The system must include the position location and identification function, a transceiver, a communications network, and a user interface. Together these elements allow for the generation, transmission, processing, and display functions that vary according to Service, hardware, resource availability, and data handling policies and protocols. Figure 2

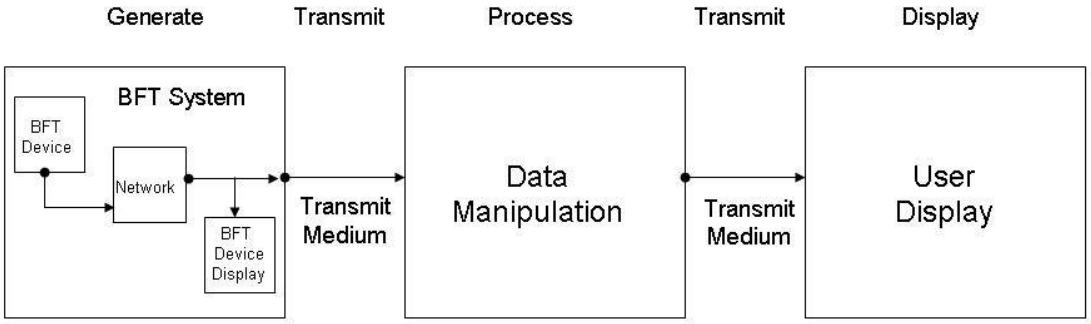

Figure 2.

graphically depicts the functional composition of a generic BFT **system** and the steps required to allow certain disparate devices to share information.[10]

Some similar devices do have the ability to communicate on a peer to peer basis, as indicated within the first block of the diagram where the generate-transmit-process-transmit-display process still occurs. These closed BFT systems require further transmission and manipulation of data in order to be shared with dissimilar devices.

Based on the figure, one can begin to get a sense for the complex nature of the systems that take BFT data and translate it into information that is readily displayed and easy to understand. It is clear that BFT technology has significant utility, but the lack of fidelity in, and enforcement of, standards to ensure interoperability has created multiple stove-piped systems which cannot communicate with one another, forming the requirement for a joint BFT capability.

Challenges

As already mentioned, there are a number of devices within the DoD inventory that generate BFT data. Historically, the Services have been responsible for designing, procuring, fielding, and sustaining their own combat gear. This Title 10 responsibility serves the individual Service well by allowing the freedom to match desired capabilities with materiel solutions. This process was sufficient in the short era of joint C2 up to and including Operation Desert Storm, where combat actions were largely de-conflicted by space and time, and Service-provided forces were able to work together through greater reliance on analog processes and segregated battlespace.

Unfortunately, Service specific requirements and acquisition processes do not facilitate joint interoperability today. The Joint Requirements Oversight Council (JROC)

was designed to address the issue of interoperability, but the initial guidance from this council was to converge existing BFT for ground forces vice develop a true joint capability.[11] Subsequent updates to the JROC have been focused on convergence only. Some progress has been made, but the task is proving more difficult than originally anticipated for a number of reasons.[12] Some are associated with technical challenges, while others are policy related issues that require difficult decisions that have yet to be made. The processes that support the JROC are prone to Service parochialism as positions are often based on program protection vice the best interests of the joint community. Consequently, the Services continue to procure devices that generate tracking information using different formats and various communication protocols.

It is also important to note that many of the devices now being used grew out of Advanced Concept Technology Demonstrations (ACTDs) vice programs of record within the Services. ACTDs are intended to exploit mature and maturing technologies to solve important military problems by allowing users to gain an understanding of proposed new capabilities for which there is no user experience base. Many devices in use today were originally provided to warfighters for evaluation.[13] They quickly saw the utility of this technology and the evaluations turned into extended operational tests that required additional devices easily procured through the ACTD construct. This got the capability fielded quickly by avoiding the normal acquisition process. Urgent Need Statements (UNS)[14] and the realities of a post “9-11” world added to this type of procurement by the Services to meet increased operational needs. Collectively, these factors have exacerbated the interoperability challenges faced today.

Once BFT data has been generated it has to be moved so that it can be manipulated into information that is useful to its consumers. This is commonly accomplished by injecting information into the common operational picture (COP) for theater wide distribution. Terrestrial based communications, like those provided by tactical radios, limit the range of communications and amount of data that can be passed. Although a few devices use this medium to transfer data, the majority use satellite-based communications that provide an over the horizon (OTH), on the move (OTM), beyond line of sight (BLOS) capability. Military and commercial satellites, to include some originally designed for use only by some of our federal agencies, are utilized primarily because of their reliability, survivability, and BLOS communications. Not all the satellites used operate within the same frequency spectrum or classification level, which complicates the engineering of solutions. The heavy reliance on space-based communications as a transport mechanism also drives up operating costs when military satellites can not be used.[15] The utilization of commercial assets is high today, and with the expected growth in tracking devices, may prove excessive in the future without improvements in moving BFT data around the battlefield. Use of commercial systems also brings up the question of susceptibility and reliability of data transmitted, particularly when those service providers are foreign owned and operated, or when intermediary network operations centers are used that are outside the military controlled domain.

An Interim Solution

The realities described above generated a need to develop a capability that could collect the various forms of BFT data, translate that data into a format that could be

widely used, and retransmit the data back to the theater from which it was generated at the desired classification level. U.S. Army Space and Missile Defense Command's Mission Management Center (MMC) in Colorado Springs has evolved from an organization originally designed to deal solely with BFT data collected by nationally controlled overhead assets, to one that can process data from all devices that generate BFT information on the battlefield today (provided adequate communication paths are in place). This is most commonly done by translating BFT data from the various devices in use into a format compatible with the Global Command and Control System (GCCS), more commonly referred to as the COP. The magnificent work performed by the professionals within this organization give commanders with access to GCCS the ability to see all BFT generated data within their area of operations.

This functional "BFT center of excellence" approach has helped to resolve many information exchange problems, but it does not completely fulfill the requirement for BFT data exchange at the lowest levels. If tactical users are not using devices that are compatible with the GCCS family of systems that normally reside at the Brigade-level and above, then they may not be able to see all devices within their area of influence.

Some argue that the cause for current interoperability challenges is lack of a single agency with direct budgetary authority over BFT system development. This may be partially to blame, but the proliferation of BFT devices can be traced to other historical reasons as well. First, no Service or CCDR truly anticipated the utility of these systems on the battlefield, which were developed to work with Service unique transmission and data distribution systems. Warfighters, policymakers, and contractors failed to recognize the impacts of digitization that started to take hold in the late 1990s and the implications

of technology when fighting in a joint environment. Although a plethora of data related standards exist to help improve interoperability, there has been little directive oversight applied to enforce adherence to standards. Service specific development efforts, ACTD procurement, and the UNS answered immediate needs, but none were concerned with interoperability across the joint community, and focused only on compatibility within a Service or unique mission domain.

Operational needs for BFT has risen exponentially since the onset of the global war on terrorism (GWOT). CCDRs, Services, and agencies have been pressing for more of these devices. This has created the need for solutions quickly, which has detracted from efforts to develop capabilities that are interoperable and joint. GPS and continued electronic advances have reduced both the time and cost of developing systems, which has in turn, driven their accelerated proliferation.

Future Requirements

Having briefly looked at the events that have transpired to date regarding blue force tracking, it is now necessary to consider emerging requirements for the future before specific recommendations on how to proceed can be made. The projected growth of devices (250,000 devices in use by 2015) will only exacerbate interoperability problems if the current way of doing business is not changed immediately. One device will not be able to satisfy all requirements, but there is a significant need for reduction in the number of systems used. Having fewer types of devices would limit the various architectures and configurations and in doing so improve interoperability. The ability of devices or systems to intercommunicate automatically facilitates both efficiency and effectiveness.[16]

A reduction in the number of systems would also improve proficiency and training efforts. Although training is adequate for the individual device, users rely heavily on contracted Field Service Representatives (FSR) for maintenance and software modifications to the systems. Training in the use of a specific system is important, but we must begin to incorporate the administrative functions into our school house curriculums as the dispersed and complex nature of future operating areas may not allow for contractor support. Maintenance and sustainability would also improve dramatically with a focused effort on fewer numbers of systems.

Commanders have advocated for the ability to “see” all friendly forces operating in their AO, and that information should be available on a single C2 display to assist in the decisionmaking processes. As the number of BFT devices and systems have grown, so too have the bandwidth and network requirements to support them. Some of these networks operate at the classified level to support BFT related missions; others work at the unclassified level. Some are designed to work with organic terrestrial based assets while more and more are migrating to satellite-based communications. These variations make it difficult for commanders to get a display that shows all blue forces operating within their AO without the service provided by the MMC. The reliance on this organization to build a comprehensive picture limits the operational flexibility of BFT.

The current National Security Strategy (NSS) and National Military Strategy (NMS) make it clear that the military must be prepared to operate in any clime and place. The ability to deploy and operate globally on short notice requires global coverage for the collection and dissemination of BFT data. Current communications architectures in place to support BFT systems can best be described as theater specific. They use

overhead assets that are often only available in that region and most require movement through a systems-specific processing or network operations center prior to being sent to the MMC. A growing majority of the overhead assets and processing centers are civilian controlled and funded through contracts executed by program managers within a Service. This too limits the operational flexibility of many BFT systems.

A joint capability also requires a new approach in the collection and dissemination of BFT-generated information. Space power is a decisive, asymmetrical advantage for our Nation, and especially for the U.S. military. But heavy reliance on overhead assets creates some vulnerability. While the United States will continue to dominate space in the near future, other nations and future adversaries are certainly not bystanders. Most potential adversaries study and understand U.S. capabilities, and strive to adapt technologies to overcome their own disadvantages. The U.S. must begin to explore communications alternatives that provide the OTM, BLOS capability desired by users within the BFT community.[17]

Information assurance of the BFT architecture is another critical requirement. There is a joint need for secured (safe) and ensured (guaranteed) communication among all friendly entities. There is also a need to ensure CCDR-controlled, unexploited access to BFT data. Network vulnerabilities that potentially provide enemy forces with this type of information must be guarded against at all costs.[18] Although the risk of exploited BFT data is low in today's operations, the proliferation of computers and ever-increasing computing power can arm potential adversaries with sophisticated tools that increase risk in this area. Technologically capable nations have conducted electronic attacks against the U.S. military and will continue to do so. The application of electronic

warfare is a very different sort of combat power which can be as lethal as kinetic fires to military and civilian targets. Computer and network attacks can reach across the world at the speed of light, invisibly targeting large masses of people in both military and civilian communities.[19] Their uniqueness requires well-considered policy as well as systems developed that can defend against attacks from packets of electrons.

The classification of the data itself plays an important role in designing the architecture to support the various systems. There is a significant policy debate ongoing within DoD regarding the proper classification of BFT data. Current interpretations of classification of data are being made from policies developed for the handling of hard-copy information routed via couriers. It is woefully inadequate in dealing with the technological advances made over the last few years in networking, communications, and electronics. The current policy development process is essentially a “political” activity, one in which the issues at hand require conciliation of diverse interests among the groups that have become identified with them.[20] This is particularly challenging as it relates to classifying BFT data because the systems were developed in a way to support the Service interpretations on the handling of data.

For example, the Army approaches the classification problem from the perspective of providing every soldier with a BFT capability in the future. Since it is an unrealistic endeavor to get every soldier a security clearance, they side on declassification of BFT data for users below the squad level. The Marine Corps believes that this data should be classified. They envision the use of both one-way (beaconing) to select individuals, and two-way (C2) devices located at key leadership positions, and view the matter of BFT information as one of disclosure that can be shared if the mission calls for it. The

combatant commands believe that classification is mission dependent, but that it should be classified when engaged in combat operations.[21] Establishing a policy on the classification of BFT data is a fundamental issue in developing a joint capability. This policy will significantly affect concept of operations, distribution of assets, and network architectures to support BFT employment.

Data exchange between devices requires network compatibility. Services face a challenge in this regard as some radios and networks employ different sets of standards. Incompatible protocols and disagreements regarding what message standards to use are significantly hampering interoperability efforts. This reality has increased complexity to our Service networks as additional translation processes have had to be added in order to share information.

The current concept of operations, or lack thereof, coupled with the rapidly growing demand for BFT has implications for the larger, joint common operational picture. GCCS is the DoD joint C2 system of record for achieving full spectrum dominance. It enhances information superiority and supports the operational concepts of full-dimensional protection and precision engagement. GCCS is the principal foundation for dominant battlespace awareness, providing an integrated, near real-time picture necessary to conduct joint and multinational operations. It is the heart of the COP. GCCS fuses select C2 capabilities into a comprehensive, interoperable system by exchanging operational and planning information to include BFT data.[22] The growing number of BFT devices alone could degrade the utility of the COP based solely on the volume of data they would produce if left unchecked. Common procedures must be developed and utilized to manage how BFT data is handled within the COP.

Recommendations

With BFT interoperability as the desired end-state, then success must come in the form of leadership, strategy, and resources. The recommendations below address each of these areas and offer specific actions for improvement and the development of a joint BFT capability.

The leadership framework is in place in the form of the Joint Requirements Oversight Council and supporting processes. As mentioned, the JROC focus has been on converging existing capabilities. As early as 2003, it became apparent that there was a need to improve efforts related to BFT interoperability.[23] Despite several JROC memorandums, limited progress has been made in reducing the variety of devices in use, or in sharing of data at the lowest levels. CJCSI 8910.01 provides Joint BFSA (JBFSA) operations guidance, but does little to define CCDR requirements.

Joint Forces Command (JFCOM), under the Joint Battle Management Command and Control (JBMC2) Roadmap, has established a JBFSA Executive Steering Committee (ESC). This organization is charged with providing leadership in developing combat effectiveness and improving interoperability and integration in this area.[24] They are currently focused on addressing previous JROC memorandums calling for the convergence of existing capabilities. Although this forum has forced compromise, it has not adequately addressed development of a joint capability. The ESC has limited ability to serve as a forcing function because members consist of Service representatives who naturally look to protect Service interests and investments. The committee has helped in identifying some of the more difficult issues for which decisions are needed, but has had limited success in forcing JROC decisions on them. Further hampering the JBFSA ESC effectiveness is the issue of Title 10 requirements versus CCDR needs.

A shift in focus is needed that will enable consideration of the critical issues at hand for a JROC decision. Such a shift would set conditions for enhanced interoperability in the future. Efforts should focus on the following:

- Breaking down the barriers of heterogeneous environments that include systems used by all military Services.
- Developing a strategy for integration and interoperability developed from the merging of CCDR and Service requirements.
- Building BFT infrastructure that supports all theaters, CCDR CONOPS, and anticipated growth across the joint spectrum.

The first step in such an effort must be the development of a concept of operations from which a BFT implementation strategy could be developed and resources applied. Former Chairman of the Joint Chiefs of Staff, Peter Pace, called for such an effort when he stated that, “The JROC should take a leading role in the formulation of CONOPS in order to help identify and fill gaps in capabilities.”[25] This is important because although various BFT CONOPS exist that are Service or theater specific, none have been developed that address all mission domains across the spectrum of conflict in a joint environment. The Chairman went on to say that developing joint concepts of operations that will be used 10, 15, 20 years out will enable the development of systems that provide these capabilities.[26]

JFCOM should lead this effort for the JROC as their mission calls for them to provide interoperable forces, develop joint enabling capabilities, and to assist leadership in making proactive, informed decisions.[27] A CONOPS that incorporates the details needed to develop a joint capability would require input from each CCDR and Service,

and should consider coalition and other government agency concerns. Each Service has estimated the number of devices required for their specific organization, but the concept of employment for these devices has not been synchronized.

JFCOM has done some work in the development of a joint CONOPS but the level of detail required in order to make policy and budgetary decisions requires additional technical expertise. A cadre of electrical engineers, computer scientists, and members of the MMC who have limited, or better yet, no habitual ties to any specific Service, is needed to augment JFCOM J85, who has done much of the heavy lifting for the JBFSA ESC. This small but skilled team should draw members from industry, the Defense Information Systems Agency (DISA), or systems engineering organizations from outside the Services.

This cadre could facilitate CONOP development by participating in the JFCOM led process with CCDRs and Services. Their expertise would serve to inform decisions regarding capabilities desired and how best to employ the technology. They could interpret and incorporate existing capabilities and concepts, and offer recommendations for how best to link requirements across mission domains. The technical focus of the cadre is needed to assist CONOP developers with issues such as device density implications to networks, security concerns and risks, and overhead resource availability. The expertise the cadre could offer would allow for the fidelity needed to identify additional issues requiring decisions and recommendations on capabilities required in a family of systems approach that meet CCDR and Services needs across all mission domains. There is no question that during this process some hard decisions will have to be made, as this approach will challenge Service positions and investments.

The cadre could serve to inform the JBFSA ESC and JROC if required on such contentious issues, and should be available to the Services to explain certain recommendations and positions in an effort to belay any fears.

DISA, the Joint Staff J-6, and Department Chief Information Officers (CIOs) all have equity in the development of network and data communication standards. Despite the great work of the individuals within these organizations, the U.S. military still develops unique systems designed to work within Service schema and architectures. The continued Service-centric development of what should be inherently joint and interdependent systems will be totally inadequate for the future. Each Service will argue that their programs adhere to published standards, but the issue of real standardization lies in the fact there is no enforcement mechanism at the joint level. Today, any Service can defend the interoperability of their programs by simply proving that they can communicate with GCCS via a habitual system relationship or through the MMC. In reality, GCCS does not reside below the Brigade level and that is exactly where interoperability efforts must be focused. A better model would be a validating function that ensures interoperability at the platform level. This needs to exist outside Service purview and within the joint realm

The previously mentioned cadre plays an important role here as well. Their alignment within JFCOM, who is responsible for the development of joint C2 systems, would allow them to provide a Service independent technical assessment, enforcing adherence to standards and protocols by Service and other tangential efforts dealing with BFT procurement. If a proposed procurement aligns with the strategy and meets the technical parameters, it would be approved. This would help in another critical area

in building a joint capability – governance. Providing recommendations rooted in adherence to technical standards at the platform level would leave little room for Service interpretation. This function becomes critical when moving from a position of trying to make Service developed systems work jointly to one that requires the systems to be born joint.

Equally important in this strategy development is the need for clear policy regarding the classification of BFT data. The fact that systems have been designed to work over an unclassified or classified network should not drive the policy. Currently, Service intelligence, information assurance, and information system experts are working this issue, and are considering a compromise where data generated from users below the squad level is considered unclassified and everything above classified.[28] This approach is short sighted as it is one that is based on current systems and will require additional protocols in the architecture to handle translations functions that complicate development and implementation efforts.

A policy must be developed that reflects the operational realities of warfare in the 21st century. Evaluating future threats and vulnerabilities to our devices, networks, and communications infrastructure will be required before any informed policy can be made. Policy should be developed from operational requirements and not from the difficulties associated with clearing all potential users or the ease associated with disclosing information. JFCOM should again lead this effort in providing the recommendation, with the JROC ultimately making the decision. Whatever the decision, it must be directive in nature to ensure joint standards are set and enforced.

A definitive policy on data classification can be worked in conjunction with a phased migration to network standards that would not only solve current BFT challenges, but interoperability on a much larger scale. Enforcement of adherence to a data classification policy could easily be incorporated into the function of the technical cadre within JFCOM. The recent call for a roles and missions review within DoD that advocates joint control of funding for command, control, computers, and communications assets presents the opportunity to enforce desperately needed governance in this area.[29]

Fiscal resources have not proven to be a challenge in procuring capability over the last six years, but this is likely to change in the future. A family of systems approach must be adopted in order to reduce the number of disparate systems currently being used to fulfill the same capability requirement. Requirements documents and contracts must be written in a way that forces interoperability. Currently, several of the devices used by DOD are produced by the same primary contractor, yet many of these devices are incapable of passing data on a peer-to-peer level. A single, family of systems contract is needed that places stringent demands on the product provider for adherence to predetermined standards and interoperability metrics. Senior leaders need to engage directly with the executives of these companies and be willing to cancel contracts if discrete interoperability metrics are not achieved. Services will argue that this approach is cost prohibitive and too time consuming, but this is in fact possible if program refresh schedules are synchronized in such a way that allow for incremental movement towards standards developed for a future BFT capability. The equipment refit issues that the Services face due to ongoing operations present an opportunity for new contracts to be

written that could improve interoperability if done correctly. There would undoubtedly be a net savings in total expenditures by adopting a family of systems approach that could be re-invested to address remaining issues such as the need for systems administration training.

A five-fold increase in the bandwidth will be needed to support BFT devices over the next five to seven years.[30] The heavy reliance on space-based communications for BFT services creates some vulnerability in the form of limited capacity and commercial reliance that must be mitigated. Alternate collection means must be explored that allow for global response as called for in the NMS. Surrogate satellite technologies that are neither theater specific nor reliant upon commercial providers to operate must be explored. These expeditionary capable devices would mitigate much of our overhead reliance on space-based assets while improving our flexibility in supporting operations around the globe.

The Defense Advanced Research Projects Agency (DARPA) has been exploring such capabilities. Airborne Communications Node (ACN) is a DARPA program to design, develop, integrate, and demonstrate a prototype communications payload for airborne platforms. It can provide enhanced theater communications capability for on-the-move warfighters. This multi-function payload enhances and augments essential warfighter communication services. One of the target platforms for the ACN payload is the Global Hawk high altitude endurance (HAE) unmanned air vehicle (UAV). Another such possible platform is the high altitude airship. ACN is not a unique, stove-piped communications capability. Rather, it enhances and augments the current mobile military communications infrastructure by working with it. It simply emulates the services

that satellites currently provide. Multiple surrogates would be required to provide the same coverage area as satellites, but it could improve intra-theater communications and inter-theater reach-back, thereby reducing the reliance on overhead national and commercial assets.

The scalability of this capability is also an attractive feature as it could be used for a small Joint Task Force (JTF) or for large scale operations. Units traditionally responsible for communications planning, installation, operations, and maintenance would manage these resources much as they do with current satellite-based systems. The senior communication organization would provide the linkage back into the DISA network. An important benefit of this technology is its ability to provide communications without the need for supporting infrastructure. It is self-deployable – at least to the extent that any airborne platform is. By loitering over the theater, it provides an instant communications capability for existing military radios on the ground, at sea, or in the air.[31] This approach could reduce the dependency on space-based assets and provide a mechanism for "theaterizing" the collection, and subsequent distribution of BFT data. It would also serve to simplify the communications architecture needed to support BFT and provide greater operational flexibility for commanders. Requirements to provide BLOS and OTH communications make it necessary to explore emerging technologies such as this. If properly resourced and considered today, it could alleviate some of our challenges and provide great operational flexibility in the future.

Conclusion

Throughout the centuries, three simple geographic location questions have been all-important to soldiers and leaders at all levels:

- "Where am I?"
- "Where are my forces and other friendly forces?"
- "Where is the enemy and what is the best route to attack him?"

Combat experience in Afghanistan and Iraq shows that BFT-equipped forces provide immediate and accurate answers to these critical location questions that have always been – and will always be – essential to decisive military operations.[32] So important is this capability that within DoD alone we will experience exponential growth in the number of devices fielded between now and 2015. The variety of devices and different capabilities they provide have created interoperability challenges that directly impact the ability to exchange this critical data at the tactical level. These challenges will increase unless a joint capability is developed that can meet all mission set requirements. A strategy developed with CCDR and Service input, coupled with informed and effective leadership and adequate resources, will set the conditions to improve interoperability of this critical capability. Hard decisions will be called for, but the young men and women who will go into harm's way in the future deserve nothing less.

Endnotes

[1] Daniel Gonzales, John Hollywood, and Sarah Harting, *Legacy Assessment of Ground Blue Force Tracking Systems* (Arlington, VA.: RAND National Defense Research Institute, 2007), 25.

[2] Bryon Greenwald, "Joint Capability Development," *Joint Forces Quarterly*, no. 44 (1st quarter 2007): 51.

[3] Chair of the Joint Chiefs of Staff Instruction 8910.01A, Joint Blue Force Situational Awareness Operations Guidance, April 30, 2004, current as of March 20, 2007, x.

[4] Lieutenant Colonel Sandy Yanna, *Comments on OUSD(AT&L)'s Legacy Assessment of Ground Blue Force Tracking Systems* (US Army Space and Missile Defense Command, Joint Blue Force Situational Awareness Mission Management Office, 2007): 2.

[5] CJCSI 8910.01A, 3.

[6] Combat Identification (CID) is the process of attaining an accurate characterization of entities in a combatant's area of responsibility to the extent that high-confidence, real-time application of tactical options and weapon resources can occur. The objective of CID is to maximize combat/mission effectiveness while reducing total casualties (due to enemy action and fractricide).

[7] Lieutenant Michael Sweeney, "Blue Force Situational Awareness Capabilty" briefing slides, HQ, U.S. Marine Corps, Arlington, Va, 30 June 2004.

[8] Gonzales, Hollywood, Harting, 17.

[9] Ibid., 15

[10] Yanna, 3.

[11] Lieutenant General James Cartwright, USMC, JROCM 161-03, Blue Force Tracking Memorandum for: Vice Chief of Staff, US Army and Assistant Commandant of the Marine Corps, The Joint Staff, Washington, D.C. 13 Aug 03

[12] Lieutenant Colonel Jim Smith, USA, Lieutenant Colonel Mike Sweeney, USMC, "Adopting Joint, Interoperability Through Convergence," Defense Acquisition University, AT&L (September – October 2005): 33 – 37.

[13] *The Joint Capability Technology Demonstrations Page,* available from http://www.acq.osd.mil/jctd; Internet; accessed 8 January, 2008.

[14] The Urgent Needs Statement process was designed to provide rapid acquisition of a capability in order to meet an urgent requirement. Resourcing of a solution is not limited to existing program of records. The acceleration of an Advanced Concept Technology Demonstration (ACTD) is often used to meet the requirement. The increased use of this process has complicated efforts to enhance interoperability.

[15] Gonzales, Hollywood, Harting, 105.

[16] Peter Anderson, Compute Systems Center Incorporated, "Systems Interoperability, MAGTF C2 Options," Quantico, Virginia, Marine Corps Combat Development Command, 16 October 2007.

[17] Lieutenant General Larry J. Dodgen, "U.S. Army, Space: Inextricably Linked to Warfighting," *Military Review* (January – February 2006): 88.

[18] Gonzales, Hollywood, Harting, 25.

[19] William J. Bayles, "The Ethics of Computer Network Attack," *Parameters (*Spring 2001): 44-46.

[20] David W. Tarr, Military Technology and the Policy Process, University of Wisconsin, 139.

[21] Joint Forces Command, “Blue Force Tracking (BFT) Position Location Information (PLI) Security and Classification Policy Briefing to the JROC,” briefing slides without scripted commentary, Pentagon, Arlington, Va., 31 January 2008.

[22] *The Defense Information Systems Agency Page,* available from http:// www.disa.mil/gccs-j/index.html; Internet; accessed 20 November 2007.

[23] JROCM 161-03 directed that the US Army and US Marine Corps develop a plan to converge existing programs of record into a single capability. Although some progress has been made in sharing data, true convergence has not been accomplished to date.

[24] *The United States Joint Forces Command Home Page,* available from http://www.jfcom.mil/about/priorities.htm; Internet; accessed 12 January, 2008.

[25] Lorenzo Cortes, “Pace Asserts JROC’s Importance in Developing CONOPS,” *Defense Daily,* (Jan 24, 2003), 1.

[26] Ibid., 1.

[27] United States Joint Forces Command, Command Mission and Strategic Goals, http://www.jfcom.mil/about/priorities.htm

[28] Joint Forces Command, “Blue Force Tracking (BFT) Position Location Information (PLI) Security and Classification Policy Briefing to the JROC,” briefing slides without scripted commentary, Pentagon, Arlington, Va., 31 January 2008.

[29] Jen DiMascio, Skelton to Press Pentagon to Start Roles and Missions Review, Defense Daily, January 24, 2008, x.

[30] Gonzales, Hollywood, Harting, 15.

[31] DARPA web site. http://www.darpa.mil/darpatech99/presentations/scripts/ato/ reichlen.we.txt

[32] Richard J. Dunn, III “Blue Force Tracking, The Afghanistan and Iraq Experience and Its Implications for the U.S. Army,” *Northrupp Grumman Mission Systems* (2005): 13.